Thank You for your purchase

Fortinet NSE5_FAZ-7.0 Exam Question & Answers

Fortinet NSE 5 - FortiAnalyzer 7.0 Exam

Product Questions: 114

Version: 6.1

Question: 1

Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains

B. Administrative access profiles

C. Trusted hosts

D. Security Fabric

Answer: BC

Explanation:

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/219292/administrator-profiles

https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts

Question: 2

Which daemon is responsible for enforcing raw log file size?

A. logfiled

B. oftpd

C. sqlplugind

D. miglogd

Answer: A

Explanation:

Question: 3

An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth
end
```

What is the significance of executing this command?

A. This command records the log file MD5 hash value.

B. This command records passwords in log files and encrypts them.

C. This command encrypts log transfer between FortiAnalyzer and other devices.

D. This command records the log file MD5 hash value and authentication code.

Answer: D

Explanation:

Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.6/administration-guide/410387/appendix-b-log-integrity-and-secure-log-transfer

Question: 4

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally?

(Choose two.)

A. Mail server

B. Output profile

C. SFTP server

D. Report scheduling

Answer: AB

Explanation:

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

Question: 5

For which two purposes would you use the command set log checksum? (Choose two.)

A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server

B. To prevent log modification or tampering

C. To encrypt log communications

D. To send an identical set of logs to a second logging server

Answer: A, B

Explanation:

To prevent logs from being tampered with while in storage, you can add a log checksum using the config

system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and

authentication code when the log is rolled and archived and when the log is uploaded (if that feature is

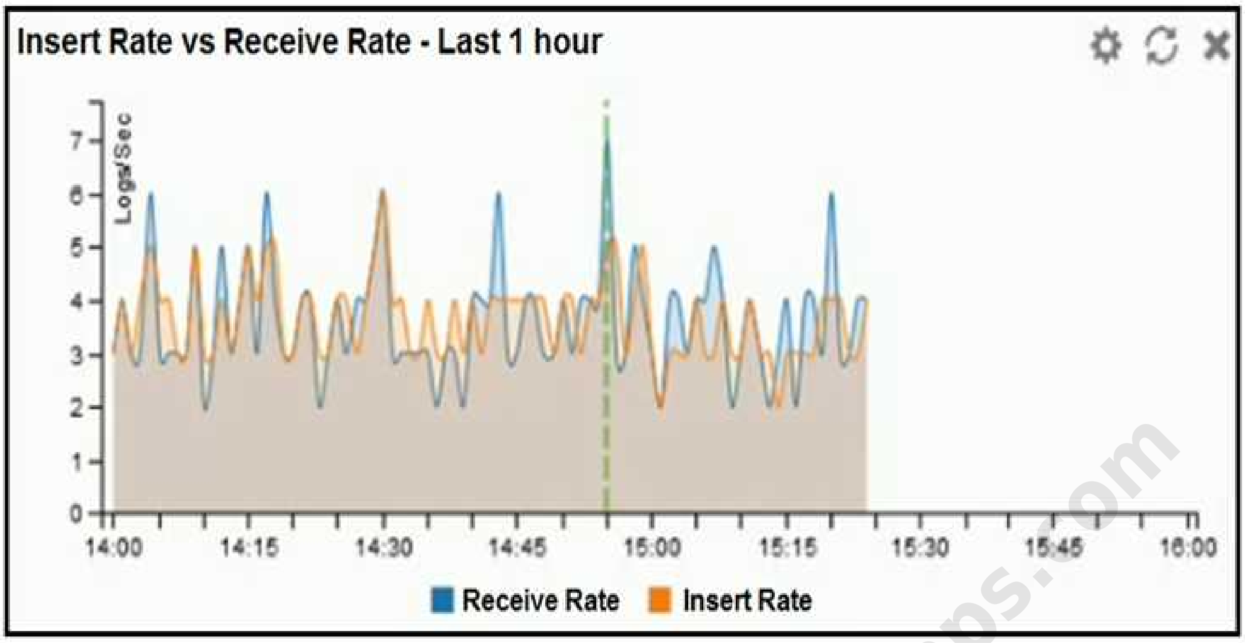
enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an

SSH File Transfer Protocol (SFTP) server during log upload.

FortiAnalyzer_7.0_Study_Guide-Online page 149

Question: 6

Refer to the exhibit.



What does the data point at 14:55 tell you?

A. The received rate is almost at its maximum for this device

B. The sqlplugind daemon is behind in log indexing by two logs

C. Logs are being dropped

D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: D

Explanation:

Question: 7

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed.

What is the recommended method to replace the disk?

A. Shut down FortiAnalyzer and then replace the disk

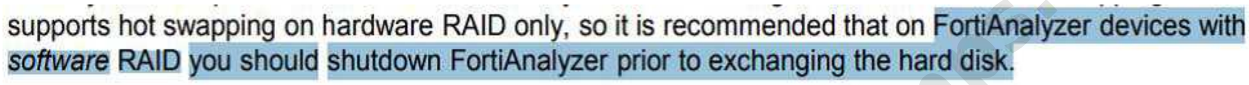
B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level

C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running

D. Perform a hot swap

Answer: A

Explanation:



supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with *software* RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

Question: 8

On the RAID management page, the disk status is listed as Initializing.

What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid

B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state

C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant

D. FortiAnalyzer is functioning normally

Answer: C

Explanation:

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4cb0dce6-dbef-11e9-

8977-00505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf (40)

Question: 9

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.

How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve

B. Configure # set resolve-ip enable in the system FortiView settings

C. Configure local DNS servers on FortiAnalyzer

D. Resolve IP addresses on FortiGate

Answer: D

Explanation:

https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/

“As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only”

Question: 10

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info

shows the quota used.

What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM

B. The maximum disk utilization for the FortiAnalyzer model

C. The maximum disk utilization for the ADOM type

D. The maximum disk utilization for all devices in the ADOM

Answer: D

Explanation:

Question: 11

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

A. To properly correlate logs

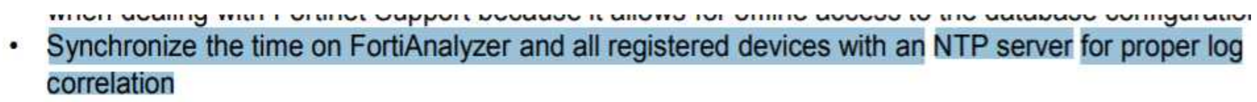
B. To use real-time forwarding

C. To resolve host names

D. To improve DNS response times

Answer: A

Explanation:



when dealing with Fortinet Support because it allows for offline access to the database configuration

- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

Question: 12

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is

temporarily unavailable?

A. FortiAnalyzer uses log fetching to retrieve the logs when back online

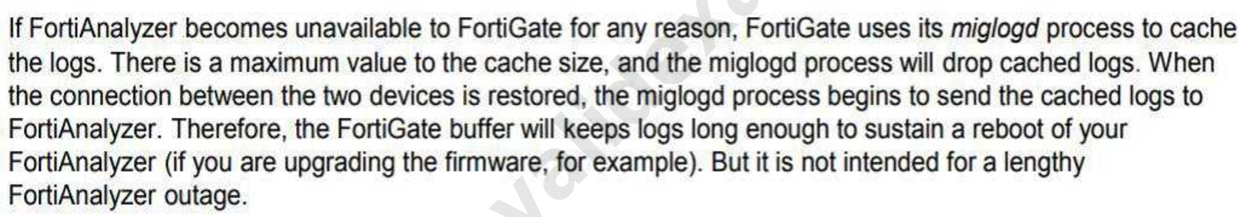
B. FortiGate uses the miglogd process to cache the logs

C. The logfiled process stores logs in offline mode

D. Logs are dropped

Answer: B

Explanation:



If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

Question: 13

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the

purpose of running the following CLI command?

execute sql-local rebuild-adom <new-ADOM-name>

A. To reset the disk quota enforcement to default

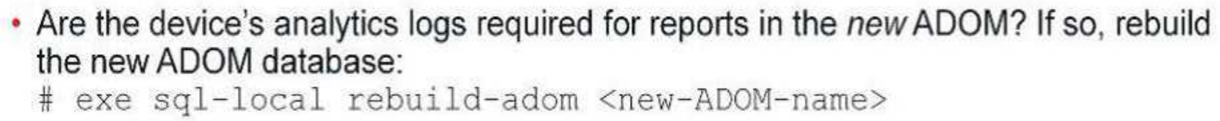
B. To remove the analytics logs of the device from the old database

C. To migrate the archive logs to the new ADOM

D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Answer: D

Explanation:



- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

Question: 14

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the

FortiAnalyzer back to functioning normally, without losing data?

A. Hot swap the disk

B. Replace the disk and rebuild the RAID manually

C. Take no action if the RAID level supports a failed disk

D. Shut down FortiAnalyzer and replace the disk

Answer: D

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

Reference: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

Question: 15

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

A. Custom datasets

B. Report scheduling

C. Report settings

D. Output profiles

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports

Question: 16

FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for

analytics logs is 60 days.

What is the most likely problem?

A. Quota enforcement is acting on analytical data before a report is complete

B. Logs are rolling before the report is run

C. CPU resources are too high

D. Disk utilization for archive logs is set for 15 days

Answer: A

Explanation:

Reference: https://forum.fortinet.com/tm.aspx?m=138806

Question: 17

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs

B. Web filter logs

C. IPS logs

D. Application control logs

Answer: B

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/

FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?

TocPath=FortiView%7CUsing%20FortiView%7C_____6

Question: 18

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

A. A local wildcard administrator account

B. A remote LDAP server

C. A trusted host profile that restricts access to the LDAP group

D. An administrator group

Answer: A, B

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567

Question: 19

When you perform a system backup, what does the backup configuration contain? (Choose two.)

A. Generated reports

B. Device list

C. Authorized devices logs

D. System information

Answer: B, D

Explanation:

https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

Reference: https://help.fortinet.com/fauth/5-2/Content/Admin%20Guides/5_2%20Admin%20Guide/300/301_Dashboard.htm

Question: 20

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

A. FROM

B. LIMIT

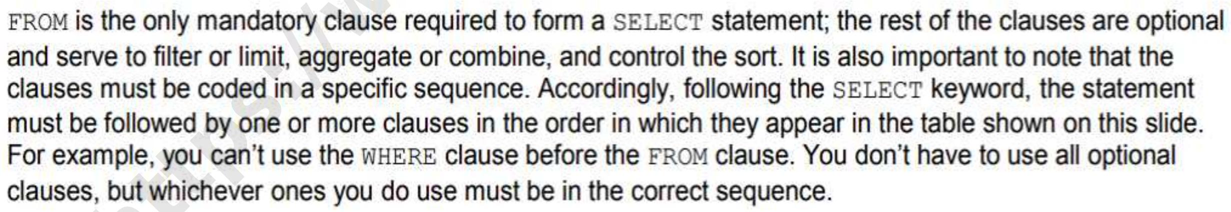
C. WHERE

D. ORDER BY

Answer: A

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500



FROM is the only mandatory clause required to form a SELECT statement; the rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide. For example, you can't use the WHERE clause before the FROM clause. You don't have to use all optional clauses, but whichever ones you do use must be in the correct sequence.

Question: 21

What is the purpose of a dataset query in FortiAnalyzer?

A. It sorts log data into tables

B. It extracts the database schema

C. It retrieves log data from the database

D. It injects log data into the database

Answer: C

Explanation:

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creating-datasets

Question: 22

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data

policy.

What is the most likely problem?

A. CPU resources are too high

B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device

C. The total disk space is insufficient and you need to add other disk

D. The ADOM disk quota is set too low, based on log rates

Answer: D

Explanation:

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device%

20logs.htm

Question: 23

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose

two.)

A. License type

B. Disk size

C. Total quota

D. RAID level

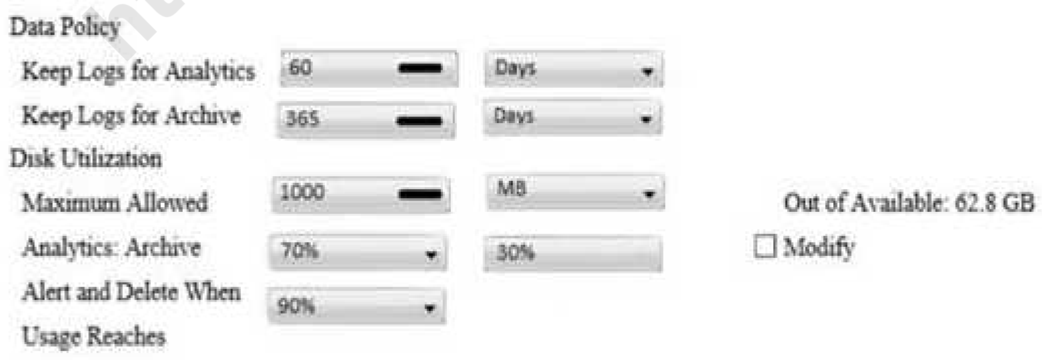
Answer: B, D

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

Question: 24

View the exhibit:



Data Policy

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

Disk Utilization

Maximum Allowed: 1000 MB   Out of Available: 62.8 GB

Analytics: Archive: 70% 30%   □ Modify

Alert and Delete When Usage Reaches: 90%

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model

B. The disk quota for all devices in the ADOM

C. The disk quota for each device in the ADOM

D. The disk quota for the ADOM type

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy

Question: 25

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

A. FortiAnalyzer resets the disk quota of the new ADOM to default.

B. FortiAnalyzer migrates archive logs to the new ADOM.

C. FortiAnalyzer migrates analytics logs to the new ADOM.

D. FortiAnalyzer removes logs from the old ADOM.

Answer: C

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

Question: 26

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log

settings?

A. The log file is stored as a raw log and is available for analytic support.

B. The log file rolls over and is archived.

C. The log file is purged from the database.

D. The log file is overwritten.

Answer: B

Explanation:

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-

81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

Question: 27

What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data

B. To provide data separation between ADOMs

C. To separate analytical and archive data

D. To back up your logs

Answer: A

Explanation:

https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%20performance%20improvement%2C%20or%20both.

Question: 28

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from

another FortiAnalyzer device?

A. Log upload

B. Indicators of Compromise

C. Log forwarding an aggregation mode

D. Log fetching

Answer: D

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

Question: 29

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage

B. From the VM host manager, expand the size of the existing virtual disk

C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk

D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Answer: A

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

Question: 30

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

D. Logs and content files are forwarded as they are received.

Answer: B

Explanation:

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes

Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-difference-between-log-forward-and-log-aggregation-modes

Question: 31

How do you restrict an administrator's access to a subset of your organization's ADOMs?

A. Set the ADOM mode to Advanced

B. Assign the ADOMs to the administrator's account

C. Configure trusted hosts

D. Assign the default Super_User administrator profile

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to-an-adom

Question: 32

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

A. Remote logging must be enabled on FortiGate

B. Log encryption must be enabled

C. ADOMs must be enabled

D. FortiGate must be registered with FortiAnalyzer

Answer: AD

Explanation:

Pg 70: “after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit.”

https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf

Pg 45: “ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox.”

Question: 33

What can the CLI command # diagnose test application oftpd 3 help you to determine?

A. What devices and IP addresses are connecting to FortiAnalyzer

B. What logs, if any, are reaching FortiAnalyzer

C. What ADOMs are enabled and configured

D. What devices are registered and unregistered

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

Question: 34

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder

B. Export to Report Chart

C. Dataset Library

D. Custom View

Answer: B

Explanation:

Question: 35

In FortiAnalyzer’s FormView, source and destination IP addresses from FortiGate devices are not resolving to

a hostname. How can you resolve the source and destination IPs, without introducing any additional

performance impact to FortiAnalyzer?

A. Configure local DNS servers on FortiAnalyzer

B. Resolve IPs on FortiGate

C. Configure # set resolve-ip enable in the system FortiView settings

D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Answer: B

Explanation:

Question: 36

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server?

(Choose two.)

A. SFTP, FTP, or SCP server

B. Mail server

C. Output profile

D. Report scheduling

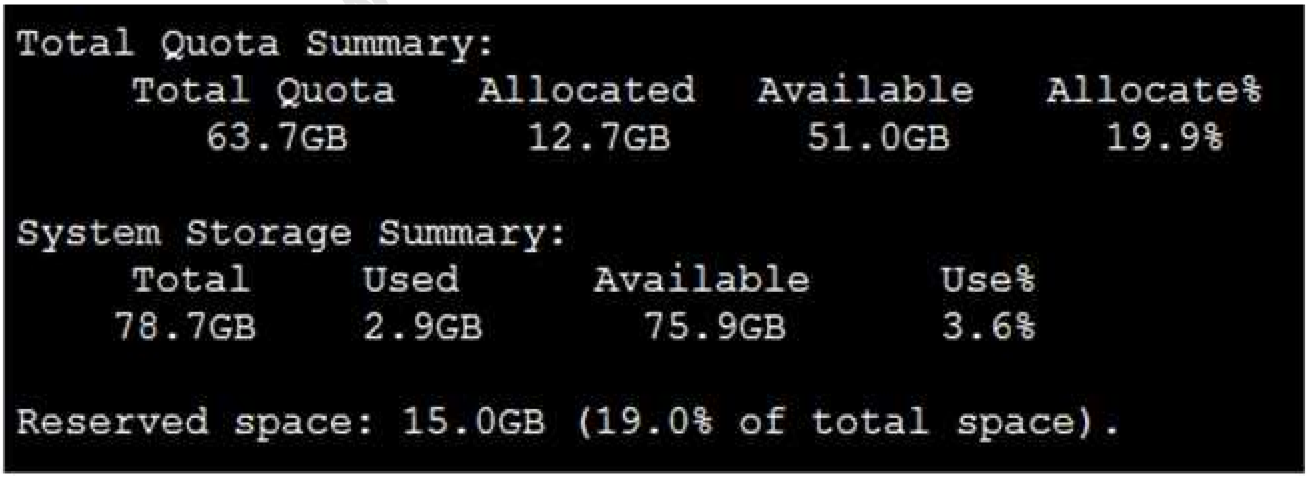
Answer: AC

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

Question: 37

View the exhibit.



```
Total Quota Summary:
     Total Quota    Allocated   Available   Allocate%
        63.7GB        12.7GB      51.0GB       19.9%

System Storage Summary:
     Total      Used        Available      Use%
    78.7GB     2.9GB         75.9GB        3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?

A. 3.6% of the system storage is already being used.

B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

C. The oftpd process has not archived the logs yet

D. The logfiled process is just estimating the total quota

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

Question: 38

What purposes does the auto-cache setting on reports serve? (Choose two.)

A. To reduce report generation time

B. To automatically update the hcache when new logs arrive

C. To reduce the log insert lag rate

D. To provide diagnostics on report generation time

Answer: AB

Explanation:

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enabling-autocache

Question: 39

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

A. Output profiles

B. Report settings

C. Report scheduling

D. Custom datasets

Answer: D

Explanation:

Question: 40

How does FortiAnalyzer retrieve specific log data from the database?

A. SQL FROM statement

B. SQL GET statement

C. SQL SELECT statement

D. SQL EXTRACT statement

Answer: A

Explanation:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b856/fortianalyzer-fortigate-sql-technote-40-mr2.pdf

Question: 41

On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of an LDAP group

B. An account that allows guest access with read-only privileges

C. An account that requires two-factor authentication

D. An account that validates against any user account on a FortiAuthenticator

Answer: A

Explanation:

https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts

Question: 42

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered

devices should:

A. Use DNS

B. Use host name resolution

C. Use real-time forwarding

D. Use an NTP server

Answer: D

Explanation:

Question: 43

What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. logfiled

B. sqlplugind

C. oftpd

D. miglogd

Answer: D

Explanation:

Reference: https://forum.fortinet.com/tm.aspx?m=143106

Question: 44

FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server

B. To prevent log modification during backup

C. To send an identical set of logs to a second logging server

D. To encrypt log communication between devices

Answer: D

Explanation:

Question: 45

How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

A. Use static routes

B. Use administrative profiles

C. Use trusted hosts

D. Use secure protocols

Answer: C

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts

Question: 46

Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

A. The total disk space is insufficient and you need to add other disk.

B. CPU resources are too high.

C. The ADOM disk quota is set too low based on log rates.

D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Answer: C

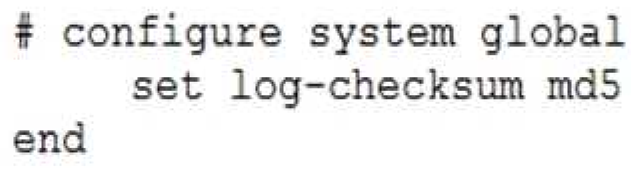
Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG
FAZ/1100_Storage/0017_Deleted%20device%20logs.htm

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

Question: 47

What is the purpose of the following CLI command?



```
# configure system global
      set log-checksum md5
end
```

A. To add a log file checksum

B. To add the MD's hash value and authentication code

C. To add a unique tag to each log to prove that it came from this FortiAnalyzer

D. To encrypt log communications

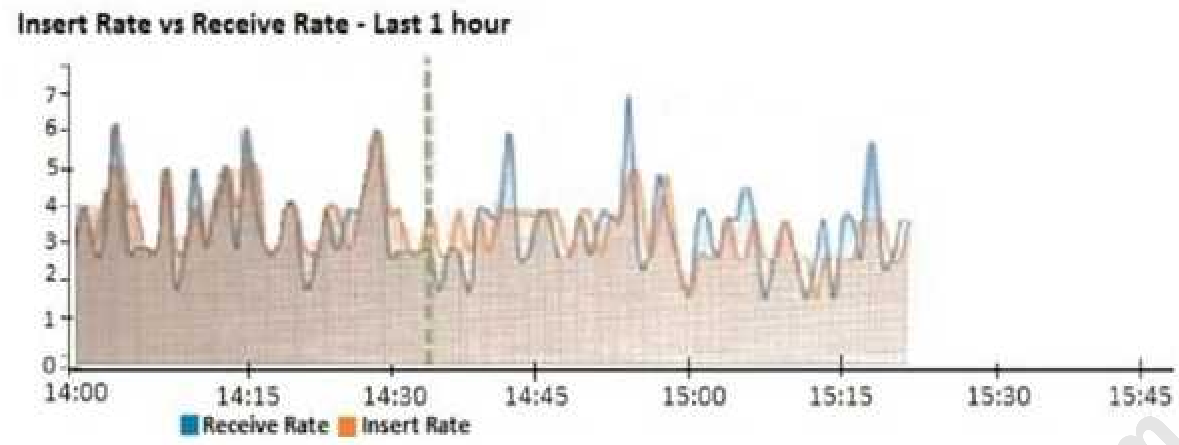
Answer: A

Explanation:

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

Question: 48

View the exhibit.



What does the data point at 14:35 tell you?

A. FortiAnalyzer is dropping logs.

B. FortiAnalyzer is indexing logs faster than logs are being received.

C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.

D. The sqlplugind daemon is ahead in indexing by one log.

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-widget

Question: 49

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

A. RADIUS

B. Local

C. LDAP

D. PKI

E. TACACS+

Answer: ACE

Explanation:

Question: 50

What statements are true regarding disk log quota? (Choose two)

A. The FortiAnalyzer stops logging once the disk log quota is met.

B. The FortiAnalyzer automatically sets the disk log quota based on the device.

C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.

D. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Answer: CD

Explanation:

Question: 51

What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

A. FortiAnalyzer distinguishes different devices by their serial number.

B. FortiAnalyzer receives logs from d devices in a duster.

C. FortiAnalyzer receives bgs only from the primary device in the cluster.

D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Answer: AB

Explanation:

Question: 52

What are the operating modes of FortiAnalyzer? (Choose two)

A. Standalone

B. Manager

C. Analyzer

D. Collector

Answer: CD

Explanation:

Question: 53

Which statements are correct regarding FortiAnalyzer reports? (Choose two)

A. FortiAnalyzer provides the ability to create custom reports.

B. FortiAnalyzer glows you to schedule reports to run.

C. FortiAnalyzer includes pre-defined reports only.

D. FortiAnalyzer allows reporting for FortiGate devices only.

Answer: A B

Explanation:

Question: 54

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

A. FortiView

B. Event Management

C. Device Manger

D. Reporting

Answer: BD

Explanation:

Question: 55

FortiAnalyzer centralizes which functions? (Choose three)

A. Network analysis

B. Graphical reporting

C. Content archiving / data mining

D. Vulnerability assessment

E. Security log analysis / forensics

Answer: BCE

Explanation:

Question: 56

By default, what happens when a log file reaches its maximum file size?

A. FortiAnalyzer overwrites the log files.

B. FortiAnalyzer stops logging.

C. FortiAnalyzer rolls the active log by renaming the file.

D. FortiAnalyzer forwards logs to syslog.

Answer: C

Explanation:

Question: 57

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.

B. ADOMs constrain other administrator’s access privileges to a subset of devices in the device list.

C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.

D. All administrators can create ADOMs--not just the admin administrator.

Answer: B,C

Explanation:

Question: 58

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.

B. SSL communications are auto-negotiated between the two devices.

C. SSL can send logs in real-time only.

D. SSL encryption levels are globally set on FortiAnalyzer.

E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Answer: A,D

Explanation:

Question: 59

What are two of the key features of FortiAnalyzer? (Choose two.)

A. Centralized log repository

B. Cloud-based management

C. Reports

D. Virtual domains (VDOMs)

Answer: A,C

Explanation:

Question: 60

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.

B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.

C. Both secure communications methods (SSL and IPsec) allow the store and upload option.

D. Disk logging is enabled on the FortiGate through the CLI only.

E. Disk logging is enabled by default on the FortiGate.

Answer: B,C,D

Explanation:

Question: 61

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.

B. Must establish an IPsec tunnel ID and pre-shared key.

C. IPsec cannot be enabled if SSL is enabled as well.

D. IPsec is only enabled through the CLI on FortiAnalyzer.

Answer: AB

Explanation:

Question: 62

Which two statements about log forwarding are true? (Choose two.)

A. Forwarded logs cannot be filtered to match specific criteria.

B. Logs are forwarded in real-time only.

C. The client retains a local copy of the logs after forwarding.

D. You can use aggregation mode only with another FortiAnalyzer.

Answer: CD

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

Question: 63

Which two methods can you use to send event notifications when an event occurs that matches a configured

event handler? (Choose two.)

A. SMS

B. Email

C. SNMP

D. IM

Answer: BC

Explanation:

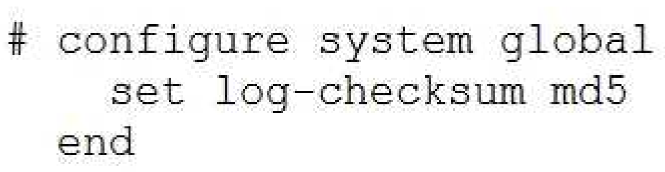
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/

FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm

Question: 64

Consider the CLI command:



```
# configure system global
    set log-checksum md5
  end
```

What is the purpose of the command?

A. To add a unique tag to each log to prove that it came from this FortiAnalyzer

B. To add the MD5 hash value and authentication code

C. To add a log file checksum

D. To encrypt log communications

Answer: C

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

Question: 65

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation

B. Host name resolution

C. Log collection

D. Real-time forwarding

Answer: A

Explanation:

Question: 66

What are two advantages of setting up fabric ADOM? (Choose two.)

A. It can be used for fast data processing and log correlation

B. It can be used to facilitate communication between devices in same Security Fabric

C. It can include all Fortinet devices that are part of the same Security Fabric

D. It can include only FortiGate devices that are part of the same Security Fabric

Answer: AC

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

Question: 67

What is the purpose of a predefined template on the FortiAnalyzer?

A. It can be edited and modified as required

B. It specifies the report layout which contains predefined texts, charts, and macros

C. It specifies report settings which contains time period, device selection, and schedule

D. It contains predefined data to generate mock reports

Answer: B

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/

2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%20number%

20of,create%20and%2For%20build%20reports.&text=A%20template%20populates%20the%20Layou t,that%

20is%20to%20be%20created.

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0010_Predefined_reports.htm

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administration-guide/618245/predefined-reports-templates-charts-and-macros

Question: 68

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal

B. Service provider

C. Identity collector

D. Identity provider

Answer: BD

Explanation:

Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/957811/saml-adminauthentication#:~:text=for%20the%20administrator.-,FortiAnalyzer%20can%20play%20the%20role%20of%

20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available.

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/981386/saml-admin-authentication

In FortiAnalyzer, SAML can be enabled across all Security Fabric devices, enabling smooth movement between devices for the administrator by means of single sign-on (SSO).

FortiAnalyzer can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP, when an external identity provider is available.

FortiAnalyzer_7.0_Study_Guide-Online pag. 48

Question: 69

Which two purposes does the auto cache setting on reports serve? (Choose two.)

A. It automatically updates the hcache when new logs arrive.

B. It provides diagnostics on report generation time.

C. It reduces the log insert lag rate.

D. It reduces report generation time.

Answer: AD

Explanation:

Reference:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache

Question: 70

What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.

B. When you restart FortiAnalyzer. all stored logs are considered to be offline logs.

C. Logs that are indexed and stored in the SQL database.

D. Logs that are collected from offline devices after they boot up.

Answer: A

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Archive_analytics_logs.htm

Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs and are considered offline so they don't offer immediate analytic support. Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data policy. FortiAnalyzer_7.0_Study_Guide-Online page 140

Question: 71

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer: B, D

Explanation:

Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.1/administration-guide/651442/fetcher-management

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

FortiAnalyzer_7.0_Study_Guide-Online pag. 168

Question: 72

An administrator has configured the following settings:

```
config system fortiview settings
set resolve-ip enable
end
```

What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.

B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.

C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.

D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer: D

Explanation:

Reference: https://community.fortinet.com/t5/Fortinet-Forum/Hostnames-in-FortiAnalyzer/m-p/95351?m=156950

Question: 73

Which two statements are true regarding ADOM modes? (Choose two.)

A. You can only change ADOM modes through CLI.

B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.

C. In an advanced mode ADOM. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.

D. Normal mode is the default ADOM mode.

Answer: CD

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/0400_ADOM%20Device%20Modes.htm

Question: 74

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.

B. In aggregation mode, you can forward logs to syslog and CEF servers as well.

C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Answer: A, C

Explanation:

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).

C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

Question: 75

An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.

What should the administrator do to solve this issue?

A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.

B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.

C. Use the execute sql-report run ADOM1 command to run a report.

D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Answer: B

Explanation:

Reference: https://help.fortinet.com/fmgr/cli/5-6-1/FortiManager_CLI_Reference/700_execute/sql-local+.htm

Question: 76

Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.

B. Macros are supported only on the FortiGate ADOM.

C. Macros are useful in generating excel log files automatically based on the reports settings.

D. Macros are predefined templates for reports and cannot be customized.

Answer: A

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

Question: 77

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

B. Collector mode is the default operating mode.

C. When in collector mode. FortiAnalyzer supports event management and reporting features.

D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

Answer: AD

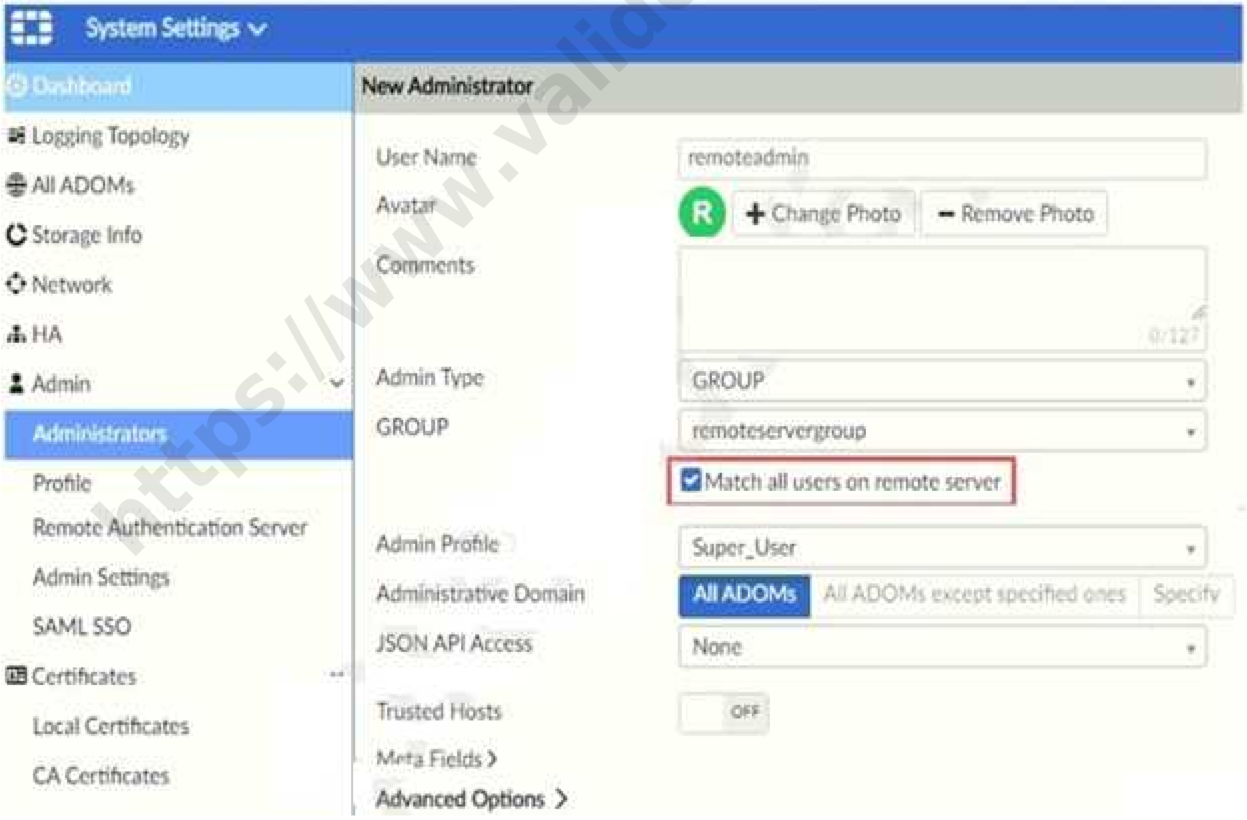
Explanation:

Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/227478/collector-mode

https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzer-collector-collaboration

Question: 78

Refer to the exhibit.



New Administrator

User Name: remoteadmin

Avatar

Comments

Admin Type: GROUP

GROUP: remoteservergroup

☑ Match all users on remote server

Admin Profile: Super_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

JSON API Access: None

Trusted Hosts: OFF

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers.

Which two statements express the significance of enabling “Match all users on remote server” when configuring a new administrator? (Choose two.)

A. It creates a wildcard administrator using LDAP and RADIUS servers.

B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.

C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.

D. It allows administrators to use two-factor authentication.

Answer: A, B

Explanation:

Reference: https://docs.fortinet.com/document/fortimanager/7.0.1/administration-guide/858351/creating-administrators

Question: 79

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.

What can you do on FortiAnalyzer to accomplish this?

A. Click FortiView and generate a report for that administrator.

B. Click Task Monitor and view the tasks performed by that administrator.

C. Click Log View and generate a report for that administrator.

D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B

Explanation:

Reference: https://docs.fortinet.com/document/fortimanager/6.4.1/administration-guide/792943/task-monitor

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 54: View the tasks FortiAnalyzer administrators have performed, including progress and status.

Question: 80

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.

What can be the reason for this failure?

A. FortiAnalyzer is in an HA cluster.

B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.

C. ADOMs are not enabled on FortiAnalyzer.

D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

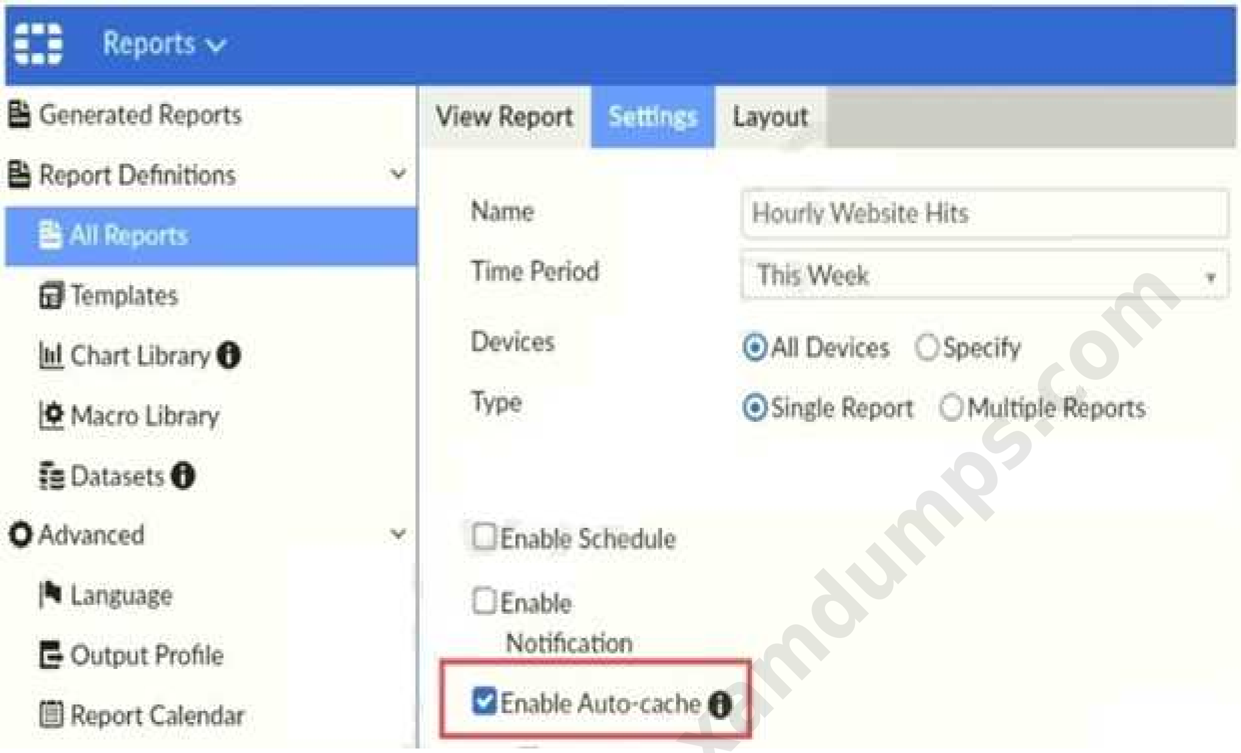
Answer: C

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

Question: 81

Refer to the exhibit.



Name: Hourly Website Hits

Time Period: This Week

Devices: ● All Devices ○ Specify

Type: ● Single Report ○ Multiple Reports

□ Enable Schedule

□ Enable Notification

☑ Enable Auto-cache

Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.

B. Reports will be cached in the memory.

C. This feature is automatically enabled for scheduled reports.

D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer: C, D

Explanation:

"Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already."

FortiAnalyzer_7.0_Study_Guide-Online page 306

Question: 82

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.

B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.

D. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: BC

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FMG-FAZ/4600_HA/0000_HA.htm?TocPath=High%20Availability%7C_____0

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

Question: 83

An administrator has moved FortiGate A from the root ADOM to ADOM1.

Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.

B. Archived logs will be moved to ADOM1 from the root ADOM automatically.

C. Logs will be presented in both ADOMs immediately after the move.

D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: B, D

Explanation:

Reference: https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between-ADOMs/m-p/32683?m=158008

Question: 84

Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.

B. Make sure all endpoints are reachable by FortiAnalyzer.

C. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.

D. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.

Answer: AD

Explanation:

In order to configure IOC, you require the following:

- A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.

- A web filter services subscription on FortiGate device(s)

- Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer

Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.

Ref : https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts

Question: 85

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.

Similarly, which feature you can use for FortiView?

A. Export to Report Chart

B. Export to PDF

C. Export to Chart Builder

D. Export to Custom Chart

Answer: A

Explanation:

Reference: https://community.fortinet.com/t5/FortiAnalyzer/Creating-a-Custom-report-from-FortiView-Export-to-Report-Chart/ta-p/190154?externalID=FD40483

Similar to the Chart Builder feature in Log View, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView. FortiAnalyzer_7.0_Study_Guide-Online pag. 292.

Question: 86

What can you do on FortiAnalyzer to restrict administrative access from specific locations?

A. Configure trusted hosts for that administrator.

B. Enable geo-location services on accessible interface.

C. Configure two-factor authentication with a remote RADIUS server.

D. Configure an ADOM for respective location.

Answer: A

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/582009/system-administrator-best-practices

Question: 87

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mall server that can be used to send email.

What could be the problem?

A. Fortinet is assigned the Standard_ User administrator profile.

B. A trusted host is configured.

C. ADOM mode is configured with Advanced mode.

D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

Explanation:

• Super_User, which, like in FortiGate, provides access to all device and system privileges.

• Standard_User, which provides read and write access to device privileges, but not system privileges.

• Restricted_User, which provides read access only to device privileges, but not system privileges. Access

to the Management extensions is also removed.

• No_Permissions_User, which provides no system or device privileges. Can be used, for example, to

temporarily remove access granted to existing admins.

FortiAnalyzer_7.0_Study_Guide-Online page 42

Question: 88

Which two statements express the advantages of grouping similar reports? (Choose two.)

A. Improve report completion time.

B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.

C. Reduce the number of hcache tables and improve auto-hcache completion time.

D. Provides a better summary of reports.

Answer: A, C

Explanation:

Question: 89

What are analytics logs on FortiAnalyzer?

A. Log type Traffic logs.

B. Logs that roll over when the log file reaches a specific size.

C. Logs that are indexed and stored in the SQL.

D. Raw logs that are compressed and saved to a log file.

Answer: C

Explanation:

Question: 90

What is Log Insert Lag Time on FortiAnalyzer?

A. The number of times in the logs where end users experienced slowness while accessing resources.

B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.

C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.

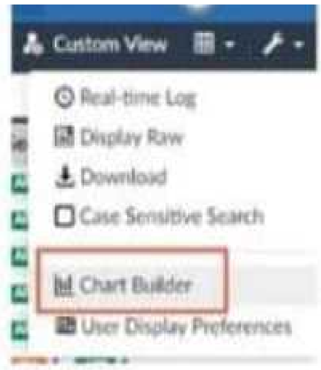
D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Answer: C

Explanation:

Question: 91

Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. In Log View, this feature allows you to build a dataset and chart automatically, based on the filtered search results.

B. In Log View, this feature allows you to build a chart and chart automatically, on the top 100 log entries.

C. This feature allows you to build a chart under FortiView.

D. You can add charts to generated reports using this feature.

Answer: A

Explanation:

Question: 92

Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

A. By default, Log Data Sync is disabled on all backup devise.

B. Log Data Sync provides real-time log synchronization to all backup devices.

C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.

D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Answer: C, D

Explanation:

Question: 93

Which two statements are true regarding fabric connectors? (Choose two.)

A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.

B. Fabric connectors allow to save storage costs and improve redundancy.

C. Storage connector service does not require a separate license to send logs to cloud platform.

D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: A, D

Explanation:

Question: 94

What does the disk status Degraded mean for RAID management?

A. One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.

B. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.

C. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.

D. The hard driveIs no longer being used by the RAID controller

Answer: D

Explanation:

Question: 95

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

A. First, upgrade the secondary device, and then upgrade the primary device.

B. Both FortiAnalyzer devices will be upgraded at the same time.

C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.

D. You can perform the firmware upgrade using only a console connection.

Answer: A

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 64: To upgrade FortiAnalyzer HA cluster firmware:

1. Log in to each secondary device.

2. Upgrade the firmware of all secondary devices.

3. Wait for the upgrades to complete and verify that all secondary devices joined the cluster.

4. Verify that logs on all secondary devices are synchronized with the primary device.

5. Upgrade the primary device.

https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

Question: 96

What is the purpose of output variables?

A. To store playbook execution statistics

B. To use the output of the previous task as the input of the current task

C. To display details of the connectors used by a playbook

D. To save all the task settings when a playbook is exported

Answer: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 242: Output variables allow you to use the output from a preceding task as an input to the current task.

"Output variables allow you to use the output from a preceding task as an input to the current task." FortiAnalyzer_7.0_Study_Guide-Online page 242

Question: 97

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information

B. Logs from registered devices

C. Report information

D. Database snapshot

Answer: AC

Explanation:

What does the System Configuration backup include?

System information, such as the device IP address and administrative user information.

Device list, such as any devices you configured to allow log access.

Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer_7.0_Study_Guide-Online pag. 29

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?

• System information, such as the device IP address and administrative user information

• Device list, such as any devices you configured to allow log access

• Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

Question: 98

Which two statements are correct regarding the export and import of playbooks? (Choose two.)

A. You can export only one playbook at a time.

B. You can import a playbook even if there is another one with the same name in the destination.

C. Playbooks can be exported and imported only within the same FortiAnaryzer.

D. A playbook that was disabled when it was exported, will be disabled when it is imported.

Answer: B, D

Explanation:

If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.

Playbooks are imported with the same status they had (enabled or disabled) when they were exported.

Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

Question: 99

Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERl'

B. SELECT devid WHERE 'u3er'='USERl' FROM $ log GROUP BY devid

C. SELECT devid FROM Slog- WHERE *user' =' USERl' GROUP BY devid

D. FROM Slog WHERE 'user* =' USERl' SELECT devid GROUP BY devid

Answer: C

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:

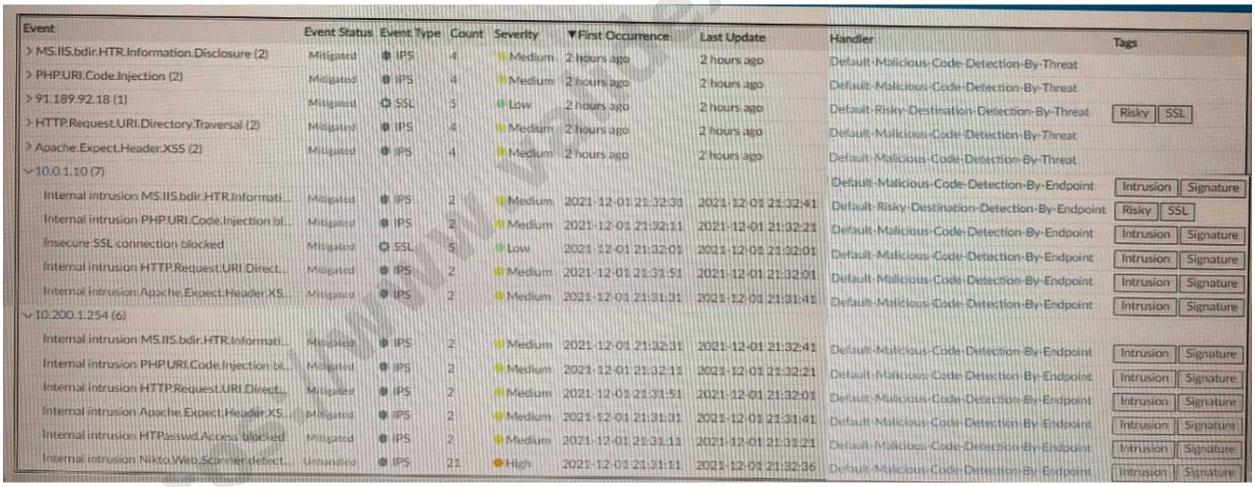
•FROM

- WHERE
- GROUP BY
- ORDER BY
- LIMIT
- OFFSET

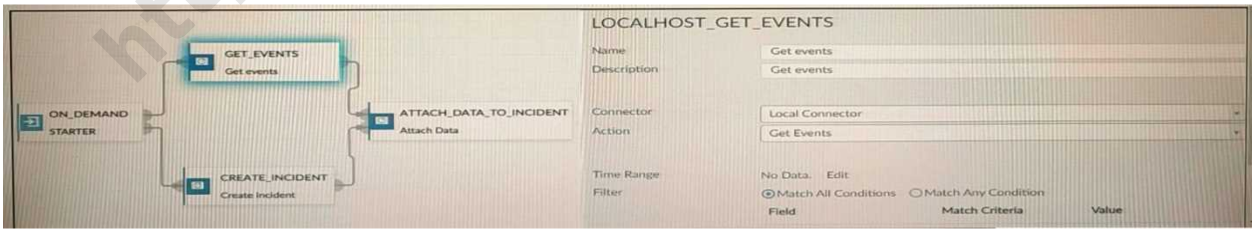
Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

Question: 100

Refer to the exhibits.



Event	Event Status	Event Type	Count	Severity	▼First Occurrence	Last Update	Handler	Tags
> MS.IIS.bdir.HTR.Information.Disclosure (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> PHP.URI.Code.Injection (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> 91.189.92.18 (1)	Mitigated	SSL	5	Low	2 hours ago	2 hours ago	Default-Risky-Destination-Detection-By-Threat	Risky SSL
> HTTP.Request.URI.Directory.Traversal (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> Apache.Expect.Header.XSS (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
∨10.0.1.10 (7)							Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Risky-Destination-Detection-By-Endpoint	Risky SSL
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Insecure SSL connection blocked	Mitigated	SSL	5	Low	2021-12-01 21:32:01	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
∨10.200.1.254 (6)								
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTPasswd.Access blocked	Mitigated	IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner.detect...	Unhandled	IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature



LOCALHOST_GET_EVENTS

Name: Get events

Description: Get events

Connector: Local Connector

Action: Get Events

Time Range: No Data. Edit

Filter: ● Match All Conditions ○ Match Any Condition

Field	Match Criteria	Value

How many events will be added to the incident created after running this playbook?

A. Ten events will be added.

B. No events will be added.

C. Five events will be added.

D. Thirteen events will be added.

Answer: A

Explanation:

Question: 101

Which daemon is responsible for enforcing the log file size?

A. sqlplugind

B. logfiled

C. miglogd

D. ofrpd

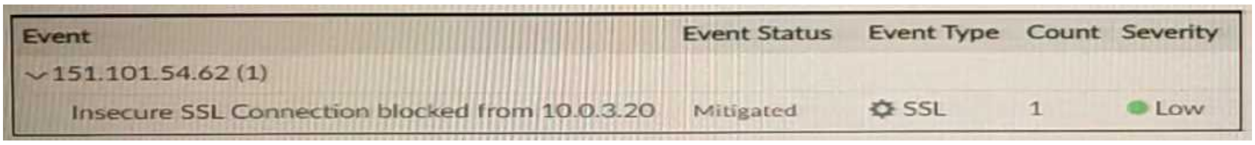
Answer: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

Question: 102

Refer to the exhibit.



Event	Event Status	Event Type	Count	Severity
∨151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙ SSL	1	● Low

Which statement is correct regarding the event displayed?

A. The security risk was blocked or dropped.

B. The security event risk is considered open.

C. An incident was created from this event.

D. The risk source is isolated.

Answer: A

Explanation:

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 206

Question: 103

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

A. A FortiGate ADOM

B. The FortiGate serial number

C. A pre-shared key

D. Valid FortiAnalyzer credentials

Answer: D

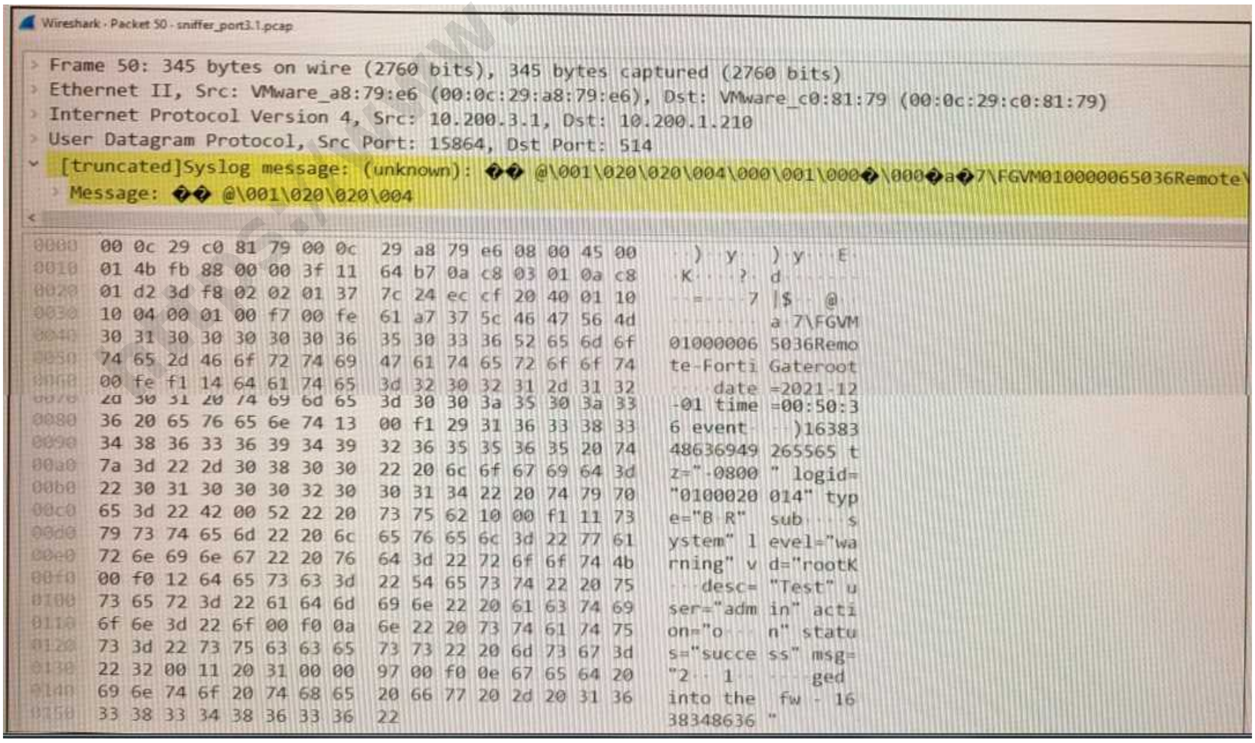
Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 93: The fourth method uses the Fortinet Security Fabric authorization process. This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

https://docs.fortinet.com/document/fortianalyzer/7.2.1/administration-guide/13897/adding-a-fortigate-using-security-fabric-authorization

Question: 104

Refer to the exhibit.



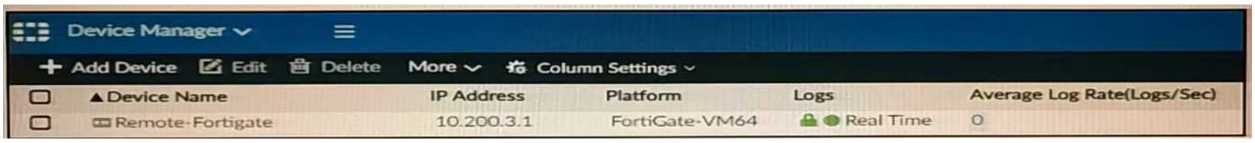
Wireshark · Packet 50 · sniffer_port3.1.pcap

```
> Frame 50: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: VMware_a8:79:e6 (00:0c:29:a8:79:e6), Dst: VMware_c0:81:79 (00:0c:29:c0:81:79)
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 15864, Dst Port: 514
v [truncated]Syslog message: (unknown): �� @\001\020\020\004\000\001\000�\000�a�7\FGVM010000065036Remote\
  > Message: �� @\001\020\020\004

0000  00 0c 29 c0 81 79 00 0c  29 a8 79 e6 08 00 45 00   ··)··y·· )·y···E·
0010  01 4b fb 88 00 00 3f 11  64 b7 0a c8 03 01 0a c8   ·K····?· d·······
0020  01 d2 3d f8 02 02 01 37  7c 24 ec cf 20 40 01 10   ··=····7 |$·· @··
0030  10 04 00 01 00 f7 00 fe  61 a7 37 5c 46 47 56 4d   ········ a·7\FGVM
0040  30 31 30 30 30 30 30 36  35 30 33 36 52 65 6d 6f   01000006 5036Remo
0050  74 65 2d 46 6f 72 74 69  47 61 74 65 72 6f 6f 74   te-Forti Gateroot
0060  00 fe f1 14 64 61 74 65  3d 32 30 32 31 2d 31 32   ····date =2021-12
0070  2d 30 31 20 74 69 6d 65  3d 30 30 3a 35 30 3a 33   -01 time =00:50:3
0080  36 20 65 76 65 6e 74 13  00 f1 29 31 36 33 38 33   6 event· ··)16383
0090  34 38 36 33 36 39 34 39  32 36 35 35 36 35 20 74   48636949 265565 t
00a0  7a 3d 22 2d 30 38 30 30  22 20 6c 6f 67 69 64 3d   z="-0800 " logid=
00b0  22 30 31 30 30 30 32 30  30 31 34 22 20 74 79 70   "0100020 014" typ
00c0  65 3d 22 42 00 52 22 20  73 75 62 10 00 f1 11 73   e="B·R"  sub····s
00d0  79 73 74 65 6d 22 20 6c  65 76 65 6c 3d 22 77 61   ystem" l evel="wa
00e0  72 6e 69 6e 67 22 20 76  64 3d 22 72 6f 6f 74 4b   rning" v d="rootK
00f0  00 f0 12 64 65 73 63 3d  22 54 65 73 74 22 20 75   ···desc= "Test" u
0100  73 65 72 3d 22 61 64 6d  69 6e 22 20 61 63 74 69   ser="adm in" acti
0110  6f 6e 3d 22 6f 00 f0 0a  6e 22 20 73 74 61 74 75   on="o··· n" statu
0120  73 3d 22 73 75 63 63 65  73 73 22 20 6d 73 67 3d   s="succe ss" msg=
0130  22 32 00 11 20 31 00 00  97 00 f0 0e 67 65 64 20   "2·· 1·· ····ged
0140  69 6e 74 6f 20 74 68 65  20 66 77 20 2d 20 31 36   into the  fw - 16
0150  33 38 33 34 38 36 33 36  22                        38348636 "
```

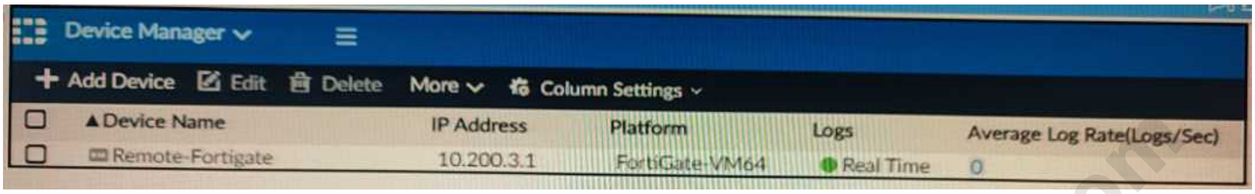
Which image corresponds to the packet capture shown in the exhibit?

A)



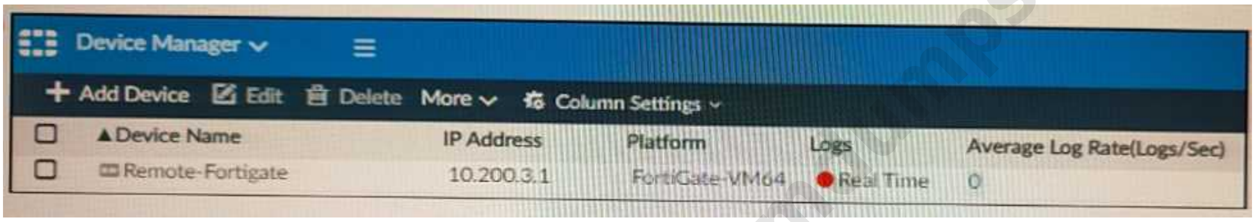
□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 🟢 Real Time	0

B)



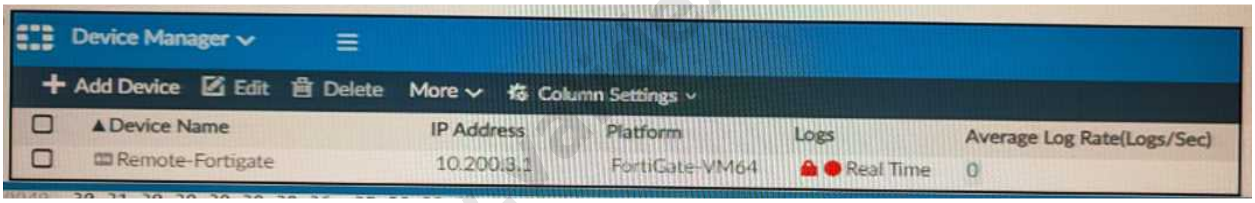
□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🟢 Real Time	0

C)



□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔴 Real Time	0

D)



□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 🔴 Real Time	0

A. Option A

B. Option B

C. Option C

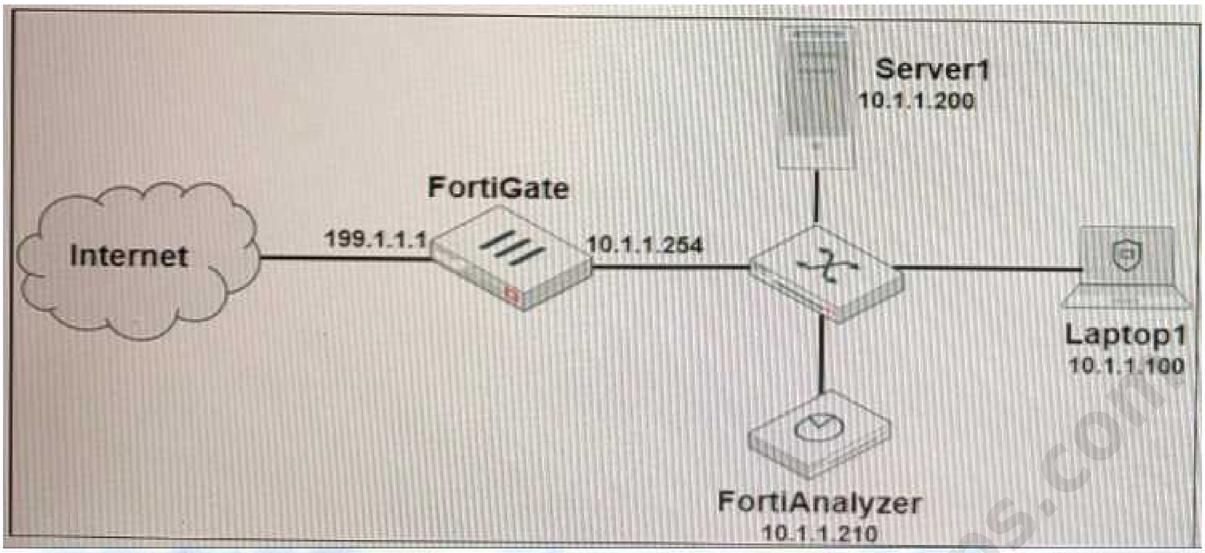
D. Option D

Answer: B

Explanation:

Question: 105

Refer to the exhibit.



Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:

Which filter will achieve the desired result?

A. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin

B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin

C. operation-login & dstip==10.1.1.210 & userl-admin

D. operation-login & performed_on=="GUI(10.1.1.210)' & user!=admin

Answer: A

Explanation:

On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

Question: 106

If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?

A. The configured IP address is checked first.

B. The active port number is checked first.

C. The firmware version is checked first.

D. The configured priority is checked first

Answer: D

Explanation:

In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:

• All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device

becomes unavailable, the device with the highest priority is selected as the new primary device. For

example, a device with a priority of 110 is selected over a device with a priority of 100.

• If multiple devices have the same priority, the device whose primary IP address has the greatest value is

selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.

• If a new device with a higher priority or a greater value IP address joins the cluster, the new device does

not replace (or pre-empt) the current primary device automatically.

FortiAnalyzer_7.0_Study_Guide-Online page 62

Question: 107

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware

RAID?

A. Hot swap the disk.

B. There is no need to do anything because the disk will self-recover.

C. Run execute format disk to format and restart the FortiAnalyzer device.

D. Shut down FortiAnalyzer and replace the disk

Answer: A

Explanation:

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0700_RAID/0800_Swapping%20Disks.htm#:~:text=If%20a%20hard%20disk%20on,to%20exchanging%20the%20hard%20disk.

Question: 108

Which statement is true about sending notifications with incident updates?

A. Notifications can be sent only when an incident is updated or deleted.

B. If you use multiple fabric connectors, all connectors must have the same notification settings

C. Notifications can be sent only by email.

D. You can send notifications to multiple external platforms

Answer: D

Explanation:

You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 34: Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates.

Question: 109

Which statement correctly describes the management extensions available on FortiAnalyzer?

A. Management extensions do not require additional licenses.

B. Management extensions allow FortiAnalyzer to act as a ForbSIEM supervisor.

C. Management extensions require a dedicated VM for best performance.

D. Management extensions may require a minimum number of CPU cores to run.

Answer: D

Explanation:

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

Question: 110

A play book contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed. What will be the status of the playbook after its execution?

A. Success

B. Failed

C. Running

D. Upstream_failed

Answer: B

Explanation:

Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. FortiAnalyzer_7.0_Study Guide page No: 247

Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. A failed status, however, does not mean that all tasks failed. Some individual actions may have been completed successfully.

Question: 111

When working with FortiAnalyzer reports, what is the purpose of a dataset?

A. To provide the layout used for reports

B. To define the chart type to be used

C. To retrieve data from the database

D. To set the data included in templates

Answer: C

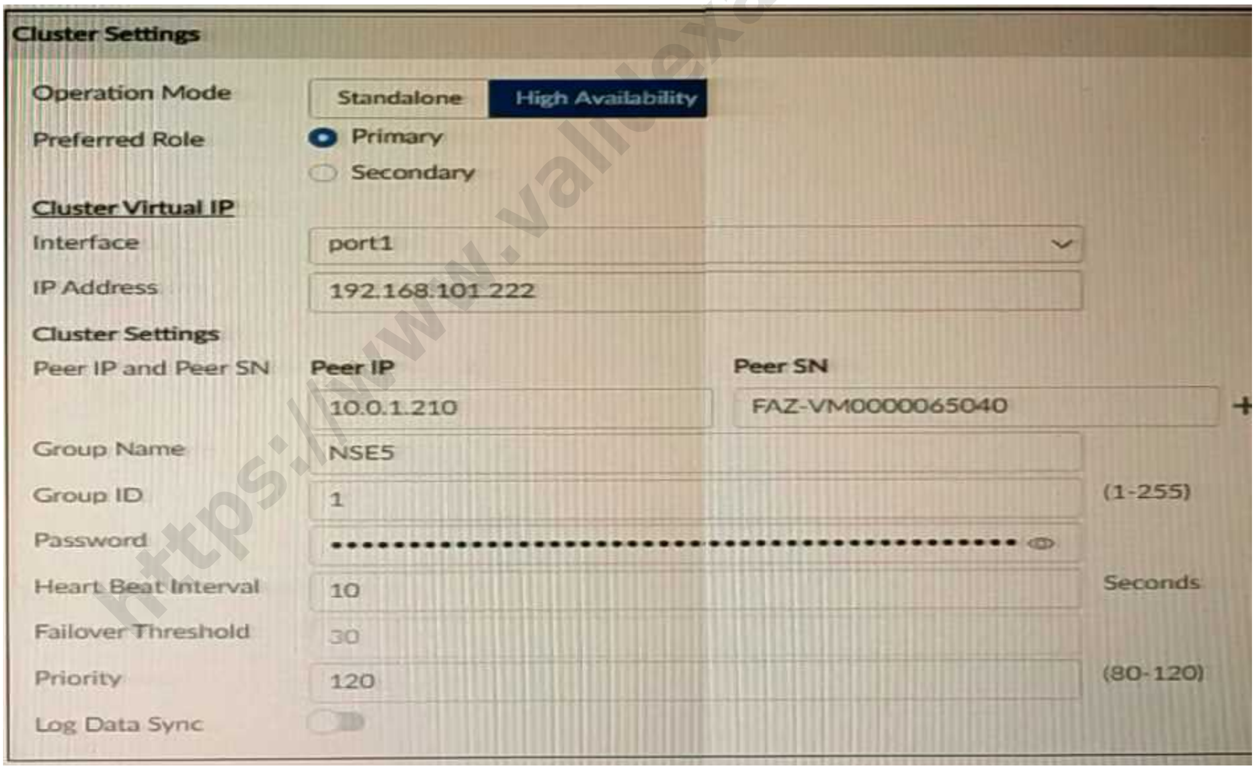
Explanation:

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creating-datasets

Datasets: Structured Query Language (SQL) SELECT queries that extract specific data from the database

Question: 112

Refer to the exhibit.



Cluster Settings

Operation Mode: Standalone | **High Availability**

Preferred Role: ● Primary ○ Secondary

Cluster Virtual IP

Interface: port1

IP Address: 192.168.101.222

Cluster Settings

Peer IP and Peer SN: Peer IP 10.0.1.210 | Peer SN FAZ-VM0000065040 +

Group Name: NSE5

Group ID: 1 (1-255)

Password: ••

Heart Beat Interval: 10 Seconds

Failover Threshold: 30

Priority: 120 (80-120)

Log Data Sync

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.

What can you conclude from the configuration displayed?

A. This FortiAnalyzer will join to the existing HA cluster as the primary.

B. This FortiAnalyzer is configured to receive logs in its port1.

C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.

D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

Answer: B

Explanation:

"If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit." (https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104)

Question: 113

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

A. FortiAnalyzer Event Handler

B. Incoming webhook

C. FortiOS Event Log

D. Fabric Connector event

Answer: B

Explanation:

"One possible scenario is shown on the slide:

1. Traffic flows through the FortiGate

2. FortiGate sends logs to FortiAnalyzer

3. FortiAnalyzer detects some suspicious traffic and generates an event

4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to

FortiGate so that it runs an automation stitch

5. FortiGate runs the automation stitch with the corrective or preventive actions"

FortiAnalyzer_7.0_Study_Guide-Online page 228

In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side. FortiAnalyzer_7.0_Study Guide page no 233

Question: 114

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. Incidents dashboards

B. Threat hunting

C. FortiView Monitor

D. Outbreak alert services

Answer: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.